JOURNAL OF NUMBER THEORY 1, 312–325 (1969)

Corresponding Residue Systems in Cyclic Extensions of Prime Degree over Algebraic Number Fields

L. R. McCULLOH

Department of Mathematics, University of Illinois, Urbana, Illinois 61801

AND

W. T. STOUT, JR.

Department of Mathematics, University of Hawaii, Honolulu, Hawaii 96822

Communicated by H. B. Mann

Received September 25, 1968

Let $\mathfrak{O}_F$ denote the ring of integers in an algebraic number field F and L/F a Galois extension. Let K and K' be intermediate fields with $K \cap K' = F$. The unique minimal ambiguous ideal $\mathfrak{A}$ of $\mathfrak{O}_L$ such that $\mathfrak{O}_K + \mathfrak{A} = \mathfrak{O}_{K'} + \mathfrak{A}$ is denoted by $\mathfrak{M}(K, K')$. It can be determined trivially unless $[K:F] = [K':F] = p^r$, a prime power. If K/F and K'/F are cyclic of prime degree p, we determine $\mathfrak{M}(K, K')$ in terms of the ramification invariants of ramified primes in L/F. For example, suppose $L = K \cdot K'$ and $\mathfrak{P}$ is a prime divisor of L, totally ramified in L/F. Let $t(L/F)$ denote the first ramification number of $\mathfrak{P}$ in L/F. Let $t = \min(t(K/F), t(K'/F))$, and $t_1 = t(L/F)$. Then $\mathfrak{M}(K, K')$ is exactly divisible by $\mathfrak{P}^M$, where $M = p(t+1) - t_1$.

INTRODUCTION

Let F be the quotient field of a Dedekind domain $\mathfrak{O}_F$. Denote (generically) by $\mathfrak{O}_L$ the integral closure of $\mathfrak{O}_F$ in a finite separable extension L of F. Throughout, we shall consider only those ideals of $\mathfrak{O}_L$ divisible by primes for which the residue class extension in L/F is separable. Let K and K' be subfields of L, with $K \cap K' = F$. For any (integral) ideal $\mathfrak{A}$ of $\mathfrak{O}_L$, we say K and K' have corresponding residue systems modulo $\mathfrak{A}$, and write $K \equiv K' \pmod{\mathfrak{A}}$, provided $\mathfrak{O}_K + \mathfrak{A} = \mathfrak{O}_{K'} + \mathfrak{A}$. Among such ideals $\mathfrak{A}$ there is a unique one minimal with respect to the property that $\mathfrak{A} = \mathfrak{A}_K \mathfrak{O}_L = \mathfrak{A}_{K'} \mathfrak{O}_L$ where $\mathfrak{A}_K = \mathfrak{A} \cap K$ and $\mathfrak{A}_{K'} = \mathfrak{A} \cap K'$. This ideal, which we denote by $\mathfrak{m}(K, K')$, is divisible only by common prime divisors

of the differents $\mathfrak{D}(K/F)$ and $\mathfrak{D}(K'/F)$. In this paper, we consider the case where K and K' are cyclic extensions of F of prime degree p and $L = K \cdot K'$. We determine $\mathfrak{m}(K, K')$ precisely in terms of ramification invariants for prime divisors of L in the extension L/F.

The notion of corresponding residue systems modulo $\mathfrak{A}$ (in the case where $\mathfrak{A} = \mathfrak{A}_K \mathfrak{O}_L = \mathfrak{A}_{K'} \mathfrak{O}_L$) was first considered by Butts and Mann [1]. In effect, they determined upper and lower bounds for $\mathfrak{m}(K, K')$ in the case where K/F and K'/F are cyclic extensions of prime degree p and F contains the pth roots of unity.

Actually, we shall consider a finer invariant associated with K and K'.

Suppose that L/F is (finite) Galois. (This is no restriction, since we may replace L by its normal closure over F in finding $\mathfrak{m}(K, K')$.) An ideal $\mathfrak{A}$ of $\mathfrak{O}_L$ is ambiguous (in L/F) if $\sigma(\mathfrak{A}) = \mathfrak{A}$ for all $\sigma \in \mathrm{Gal}(L/F)$, the Galois group of L over F. Among the ambiguous ideals $\mathfrak{A}$ of $\mathfrak{O}_L$ such that $K \equiv K' \pmod{\mathfrak{A}}$, there is a unique minimal one which is the lowest common multiple of the others. (If one does not restrict attention to ambiguous ideals, no such minimal ideal exists in general.) This ideal, which we denote by $\mathfrak{M}(K, K')$, is divisible only by primes $\mathfrak{P}$ of L, totally ramified in K/F and in K'/F. (By this, we mean that $\mathfrak{P}_K$ and $\mathfrak{P}_{K'}$ are totally ramified over $\mathfrak{P}_F$, where we generically denote by $\mathfrak{P}_K$ the prime divisor $\mathfrak{P} \cap K$ of K.) The smallest ideal $\mathfrak{A}$ of $\mathfrak{O}_L$ containing $\mathfrak{M}(K, K')$ and having the form $\mathfrak{A} = \mathfrak{A}_K \mathfrak{O}_L = \mathfrak{A}_{K'} \mathfrak{O}_L$ is $\mathfrak{m}(K, K')$.

In Section 1, we derive some general facts about corresponding residue systems and show that the problem of determining $\mathfrak{M}(K, K')$ can be "semi-localized" to the problem of determining for each prime $\mathfrak{p}$ of F the contribution $\mathfrak{M}(\mathfrak{p} : K, K')$ of the prime factors of $\mathfrak{p}$ in L. For this, one can replace $\mathfrak{O}_F$ by the valuation ring in F associated with $\mathfrak{p}$. We also show that the determination of $\mathfrak{M}(K, K')$ is trivial unless $[K : F] = [K' : F] = p^r$, a prime power. (The problem becomes interesting only when there is higher (wild) ramification.) This was shown for $\mathfrak{m}(K, K')$ by Butts and Mann [1] in the case where K/F and K'/F are normal extensions. It is not entirely trivial to remove the restriction of normality. Most of the other results of this section are, however, easy generalizations of those of [1].

In Section 2, we impose the restriction that K/F and K'/F be normal extensions and for convenience, we assume $L = K \cdot K'$, the composite. We determine $\mathfrak{M}(\mathfrak{p} : K, K')$ under the assumption that the prime $\mathfrak{p}$, which is totally ramified in K/F (and K'/F), does not ramify further in L/K (and L/K'). (This result includes the cases considered in [1, Theorems 11 and 15].)

$\mathfrak{M}(K, K')$ is determined in Section 3 in the case that K/F and K'/F are cyclic extensions of degree p, and we recover and improve in Section 4 certain results of [1] for the case that F contain the pth roots of unity.

1. General Results

Let L/F be finite Galois and let K and K' be subfields of L with $K \cap K' = F$. Let $\mathfrak{A}$ be an ideal of $\mathfrak{O}_L$. We begin by deriving several necessary conditions for $K \equiv K' \pmod{\mathfrak{A}}$.

(1.1) Proposition. *Suppose* $K \equiv K' \pmod{\mathfrak{A}}$. *Let* $\mathfrak{A}_K = \mathfrak{A} \cap K$ *and* $\mathfrak{A}_{K'} = \mathfrak{A} \cap K'$. *Then* $\mathfrak{A}_K$ *and* $\mathfrak{A}_{K'}$ *have corresponding prime factorizations*:

$$\mathfrak{A}_K = \prod \{\mathfrak{p}_i^{t_i} : i = 1, \ldots, s\}$$

$$\mathfrak{A}_{K'} = \prod \{\mathfrak{p}_i'^{t_i} : i = 1, \ldots, s\}$$

where the $\mathfrak{p}_i$(resp $\mathfrak{p}_i'$) *are distinct prime ideals of* $\mathfrak{O}_K$(resp $\mathfrak{O}_{K'}$). *For the corresponding prime ideals we have*

(i) $\mathfrak{p}_i + \mathfrak{A} = \mathfrak{p}_i' + \mathfrak{A}$.

(ii) $\mathfrak{p}_i = (\mathfrak{p}_i' + \mathfrak{A}) \cap \mathfrak{O}_K$ *and* $\mathfrak{p}_i' = (\mathfrak{p}_i + \mathfrak{A}) \cap \mathfrak{O}_{K'}$.

(iii) $\mathfrak{p}_i$ *and* $\mathfrak{p}_i'$ *lie over the same prime ideal of* $\mathfrak{O}_F$ *with the same residue class degrees* $f(\mathfrak{p}_i : K/F) = f(\mathfrak{p}_i' : K'/F)$.

First we note the following well-known facts:

(1.2) Proposition. *If* $g : R \to \bar{R}$ *is a ring homomorphism from a Dedekind domain* R *onto a ring* $\bar{R}$ *with* $\ker g = \mathfrak{a} \neq (0)$, *then the canonical correspondence* $\mathfrak{b} \leftrightarrow \bar{\mathfrak{b}}$ *between ideals of* R *containing* $\mathfrak{a}$ *and ideals of* $\bar{R}$ *associates prime divisors* $\mathfrak{p}$ *of* $\mathfrak{a}$ *with maximal ideals* $\bar{\mathfrak{p}}$ *of* $\bar{R}$. *If* $\mathfrak{p}^e | \mathfrak{a}$ *but* $\mathfrak{p}^{e+1} \nmid \mathfrak{a}$ (here, $|$ means "divides"), *then* e *is the smallest integer such that* $\bar{\mathfrak{p}}^e = \bar{\mathfrak{p}}^{e+1}$. *Also* $R/\mathfrak{p} \cong \bar{R}/\bar{\mathfrak{p}}$. (*From this, it follows that the prime factorization of* $\mathfrak{a}$ *and the residue class fields of the primes dividing* $\mathfrak{a}$ *are determined entirely by properties of* $\bar{R}$.)

Proof. We remark only that the standard correspondence is multiplicative in the sense that if $\mathfrak{b} \leftrightarrow \bar{\mathfrak{b}}$ and $\mathfrak{b}' \leftrightarrow \bar{\mathfrak{b}}'$, then $\mathfrak{b} \cdot \mathfrak{b}' + \mathfrak{a} \leftrightarrow \bar{\mathfrak{b}} \cdot \bar{\mathfrak{b}}'$. The rest is an easy exercise.

Proof of (1.1). One applies (1.2) to the canonical homomorphisms $g : \mathfrak{O}_K \to \mathfrak{O}_L/\mathfrak{A}$ and $g' : \mathfrak{O}_{K'} \to \mathfrak{O}_L/\mathfrak{A}$, noting that $\ker g = \mathfrak{A}_K$ and $\ker g' = \mathfrak{A}_{K'}$. The assumption that $K \equiv K' \pmod{\mathfrak{A}}$ implies that $g(\mathfrak{O}_K) = g'(\mathfrak{O}_{K'})$. But since the factorization of the kernel is determined by properties of the image ring, it follows that $\mathfrak{A}_K$ and $\mathfrak{A}_{K'}$ have corresponding prime factorizations as asserted. The statements (i) and (ii) are merely translations of the statements $g(\mathfrak{p}_i) = g'(\mathfrak{p}_i') = \bar{\mathfrak{p}}_i$ and $\mathfrak{p}_i = g^{-1}(\bar{\mathfrak{p}}_i)$ and $\mathfrak{p}_i' = g'^{-1}(\bar{\mathfrak{p}}_i)$. Finally, (iii) is an easy consequence of $g(\mathfrak{O}_F) = g'(\mathfrak{O}_F)$.

We remark that if $\mathfrak{A} = \mathfrak{A}_K \mathfrak{O}_L = \mathfrak{A}_{K'} \mathfrak{O}_L$ (as considered in [1]), the

prime factorizations are identical in the sense that $\mathfrak{p}_i\mathfrak{O}_L = \mathfrak{p}_i'\mathfrak{O}_L$. For in that case $\mathfrak{p}_i\mathfrak{O}_L \supseteq \mathfrak{A}$ and $\mathfrak{p}_i'\mathfrak{O}_L \supseteq \mathfrak{A}$ so that

$$\mathfrak{p}_i\mathfrak{O}_L = (\mathfrak{p}_i+\mathfrak{A})\mathfrak{O}_L = (\mathfrak{p}_i'+\mathfrak{A})\mathfrak{O}_L = \mathfrak{p}_i'\mathfrak{O}_L.$$

(1.3) PROPOSITION. *Suppose* $\mathfrak{A}$ *is ambiguous in* L/F *and that* $K \equiv K' \pmod{\mathfrak{A}}$. *Then, for all* $\sigma \in \mathrm{Gal}(L/F)$ *and all* $\alpha \in \mathfrak{O}_K \cdot \mathfrak{O}_{K'}$ *we have* $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{A}}$. (*This does not generally hold for all* $\alpha \in \mathfrak{O}_L$.)

Proof. Let $\mathfrak{O} = \mathfrak{O}_K + \mathfrak{A} = \mathfrak{O}_{K'} + \mathfrak{A}$. ($\mathfrak{O}$ is a subring of $\mathfrak{O}_L$, indeed it is an $\mathfrak{O}_F$-order of L.) Clearly $\mathfrak{O}_K \cdot \mathfrak{O}_{K'} \subseteq \mathfrak{O}$. Let $H = \{\sigma \in \mathrm{Gal}(L/F) : (\sigma-1)\mathfrak{O} \subseteq \mathfrak{A}\}$. Since $\mathfrak{A}$ is ambiguous, H is a subgroup. For $\sigma, \tau \in H$ implies

$$(\sigma\tau-1)\mathfrak{O} \subseteq (\sigma\tau-\sigma)\mathfrak{O} + (\sigma-1)\mathfrak{O} \subseteq \sigma\mathfrak{A} + \mathfrak{A} = \mathfrak{A}.$$

Moreover $\mathrm{Gal}(L/K) \subseteq H$. For $\sigma \in \mathrm{Gal}(L/K)$ implies that $(\sigma-1)\mathfrak{O}_K = \{0\}$ whence $(\sigma-1)(\mathfrak{O}_K+\mathfrak{A}) = (\sigma-1)\mathfrak{A} \subseteq \mathfrak{A}$. Similarly, $\mathrm{Gal}(L/K') \subseteq H$, so $H = \mathrm{Gal}(L/F)$ and the result follows.

The preceding proposition has numerous consequences which we shall consider later. For now, it will suffice to observe that it implies that $\mathfrak{A}$ cannot be arbitrarily small. For if we choose $\alpha \in \mathfrak{O}_K$, $\alpha \notin F$, then $\mathfrak{A} \supseteq (\alpha-\alpha')\mathfrak{O}_L$ where α' is any conjugate of α over F. Thus we have shown the existence of a minimal ambiguous $\mathfrak{A}$ such that $K \equiv K' \pmod{\mathfrak{A}}$. The next proposition will guarantee its uniqueness.

(1.4) PROPOSITION. *Suppose* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are ambiguous ideals of* $\mathfrak{O}_L$ *and are relatively prime* (i.e. $\mathfrak{A}+\mathfrak{B} = \mathfrak{O}_L$). *If* $K = K' \pmod{\mathfrak{A}}$ *and* $K \equiv K' \pmod{\mathfrak{B}}$, *then* $K = K' \pmod{\mathfrak{AB}}$.

Proof. Let $\gamma' \in \mathfrak{O}_{K'}$. Then we have $\gamma' \equiv \alpha \pmod{\mathfrak{A}}$ and $\gamma' \equiv \beta \pmod{\mathfrak{B}}$ for suitable $\alpha, \beta \in \mathfrak{O}_K$. Now, since $\mathfrak{A}$ and $\mathfrak{B}$ are ambiguous and relatively prime, $\mathfrak{A}_K$ and $\mathfrak{B}_K$ are relatively prime. Thus, by the Chinese remainder theorem, there is a $\gamma \in \mathfrak{O}_K$ such that $\alpha \equiv \gamma \pmod{\mathfrak{A}_K}$ and $\beta \equiv \gamma \pmod{\mathfrak{B}_K}$. Hence $\gamma' \equiv \gamma \pmod{\mathfrak{A}}$ and $\gamma' \equiv \gamma \pmod{\mathfrak{B}}$. Again, since $\mathfrak{A}$ and $\mathfrak{B}$ are coprime, $\gamma' \equiv \gamma \pmod{\mathfrak{AB}}$. Thus, $\mathfrak{O}_{K'} \subseteq \mathfrak{O}_K + \mathfrak{AB}$, which suffices by symmetry.

(1.5) DEFINITION. Let $\mathfrak{M}(K, K')$ denote the (unique) minimal ambiguous ideal $\mathfrak{A}$ of $\mathfrak{O}_L$ such that $K \equiv K' \pmod{\mathfrak{A}}$. We note that $\mathfrak{M}(K, K')$ is divisible by all other such ambiguous ideals. (The dependence of $\mathfrak{M}(K, K')$ on the choice of field L containing K and K' is suppressed since it is only superficial. Evidently if we replace L by a larger field L', finite Galois over F, then $\mathfrak{M}(K, K')$ is replaced merely by $\mathfrak{M}(K, K') \cdot \mathfrak{O}_{L'}$.)

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_F$ and $\mathfrak{P}$ a prime divisor of L, dividing $\mathfrak{p}$. Let $\mathfrak{P}^\#$ denote the product of the distinct conjugates of $\mathfrak{P}$ over F. Then $\mathfrak{p}\cdot\mathfrak{O}_L = (\mathfrak{P}^\#)^e$ where $e = e(\mathfrak{P}; L/F)$ is the ramification index of $\mathfrak{P}$ over F.

We shall (generically) denote by w_K the normalized additive valuation of K for the prime $\mathfrak{P}_K$.

(1.6) DEFINITION. Let $\mathfrak{M}(\mathfrak{p} : K, K')$ denote the $\mathfrak{p}$-component of $\mathfrak{M}(K, K')$. We note that, in view of (1.4), $\mathfrak{M}(\mathfrak{p} : K, K') = (\mathfrak{P}^\#)^M$ where $M = M(\mathfrak{P}^\# : K, K')$ is the largest integer for which $K \equiv K' \pmod{(\mathfrak{P}^\#)^M}$.

Let

$$n = [K : F] \quad \text{and} \quad n' = [K' : F].$$

(1.7) THEOREM. *$K \equiv K' \pmod{\mathfrak{P}^\#}$ if and only if $\mathfrak{P}$ is totally ramified in K/F and in K'/F. Furthermore, in this case $M(\mathfrak{P}^\# ; K, K') \geq \min(e/n, e/n')$, and equality holds if $n \neq n'$.*

Proof. First suppose $\mathfrak{P}$ is totally ramified in K/F and K'/F. Then $(\mathfrak{P}^\#)^{e/n} = \mathfrak{P}_K\cdot\mathfrak{O}_L$ and $(\mathfrak{P}^\#)^{e/n'} = \mathfrak{P}_{K'}\cdot\mathfrak{O}_L$. Suppose $n \geq n'$. We must show $K \equiv K' \pmod{(\mathfrak{P}^\#)^{e/n}}$.

Since the residue class degree $f(\mathfrak{P}_K; K/F) = 1$, we have $\mathfrak{O}_K = \mathfrak{O}_F + \mathfrak{P}_K$. Likewise $\mathfrak{O}_{K'} = \mathfrak{O}_F + \mathfrak{P}_{K'}$. Now $\mathfrak{P}_K \subseteq (\mathfrak{P}^\#)^{e/n}$ and $\mathfrak{P}_{K'} \subseteq (\mathfrak{P}^\#)^{e/n}$. Hence, adding $(\mathfrak{P}^\#)^{e/n}$ to both sides of the above equation we obtain

$$\mathfrak{O}_K + (\mathfrak{P}^\#)^{e/n} = \mathfrak{O}_F + (\mathfrak{P}^\#)^{e/n} = \mathfrak{O}_{K'} + (\mathfrak{P}^\#)^{e/n},$$

whence $M(\mathfrak{P}^\# : K, K') \geq e/n$. Moreover, if $n > n'$, then $(\mathfrak{P}^\#)^{(e/n)+1} \cap K = \mathfrak{P}_K^2$ while $(\mathfrak{P}^\#)^{(e/n)+1} \cap K' = \mathfrak{P}_{K'}$. Thus, if $K \equiv K' \pmod{(\mathfrak{P}^\#)^{(e/n)+1}}$, the requirement of corresponding prime factorizations of (1.1) would be violated. Hence $M(\mathfrak{P}^\# : K, K') = e/n$.

Conversely, suppose $K \equiv K' \pmod{\mathfrak{P}^\#}$. By symmetry, it suffices to show $\mathfrak{P}$ totally ramified in K/F. First, we show that $\mathfrak{p}$ does not split in K/F. Let $\sigma \in \mathrm{Gal}(L/F)$, and $\alpha \in \mathfrak{P}_K \subseteq \mathfrak{P}$. By (1.3), $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^\#}$. Therefore, $\sigma(\alpha) \equiv 0 \pmod{\mathfrak{P}}$. Hence $\mathfrak{P} \supseteq \sigma(\mathfrak{P}_K)$ or $\sigma^{-1}(\mathfrak{P}) \supseteq \mathfrak{P}_K$. Hence $\mathfrak{P}_K$ is divisible by all conjugates of $\mathfrak{P}$ in L/F, so $\mathfrak{p}$ does not split in K/F.

It remains to show $f(\mathfrak{P}_K; K/F) = 1$. Now, $\mathfrak{O}_L/\mathfrak{P}$ is a Galois extension of $\mathfrak{O}_F/\mathfrak{p}$, and all automorphisms are induced by automorphisms in $\mathrm{Gal}(L/F)$ (or, more precisely, in the decomposition group of $\mathfrak{P}$ in L/F). But, by (1.3), elements of $\mathfrak{O}_K$ are left fixed (mod $\mathfrak{P}$) by such automorphisms. Hence $\mathfrak{O}_K/\mathfrak{P}_K$ is fixed elementwise by all automorphisms of $\mathfrak{O}_L/\mathfrak{P}$ over $\mathfrak{O}_F/\mathfrak{p}$. Thus $f(\mathfrak{P}_K; K/F) = 1$, as required.

The preceding theorem completely determines $\mathfrak{M}(K, K')$ in case $[K : F] \neq [K' : F]$. Now, suppose $n = [K : F] = [K' : F]$.

(1.8) THEOREM. *Suppose $\mathfrak{P}$ is totally ramified in K/F and K'/F. Then $M(\mathfrak{P}^{\#}; K, K') \geq e/n$. Here, equality holds unless $n = p^r$ for some r, where p is the rational prime divisible by $\mathfrak{P}$* (i.e. *the residue class characteristic of $\mathfrak{P}$*).

Before proving Theorem (1.8), we state the following proposition which will be used in the proof. Denote by $\Gamma(K \to L; F)$ the set of F-isomorphisms of K into L. (There are $[K:F]$ such isomorphisms.)

(1.9) PROPOSITION. *Let $\mathfrak{P}$ be totally ramified in the extension K/F, and let $F \subseteq E \subseteq K$. Let π_K be a prime element for $\mathfrak{P}_K$ in K and π_E a prime element for $\mathfrak{P}_E$ in E. Let $\sigma \in \Gamma(E \to L; F)$. Then*

$$w_L(\sigma(\pi_E) - \pi_E) = \sum_{s \to \sigma} w_L(s(\pi_K) - \pi_K)$$

where the index s of the summation runs over the set of those $s \in \Gamma(K \to L; F)$ whose restriction to E coincides with σ.

We omit the proof. In essence, this proposition is the same as ([4], Proposition 3, p. 71). Although it is stated there with the additional assumptions that K/F and E/F are Galois and that K is complete, these assumptions are not essential to the proof given there.

Proof of (1.8). We know from (1.7) that $M(\mathfrak{P}^{\#}; K, K') \geq e/n$. Suppose $>$ holds. Let $n = e_0 \cdot p^r$ where $p \nmid e_0$. We must show $e_0 = 1$.

Let $N \subseteq L$ be the normal closure of K over F. Let T and V denote, respectively, the inertia and (first) ramification fields for $\mathfrak{P}_N$ in N/F. Since $\mathfrak{P}$ is unramified in T/F and totally ramified in K/F, the two extensions are linearly disjoint, which is to say that $[KT:T] = [K:F] = e_0 p^r$. Now, since N/T is Galois and $\mathfrak{P}$ is totally ramified in N/T, the Galois group of N/T is unchanged if N and T are replaced by their completions at $\mathfrak{P}$. In particular, the lattice of fields between N and T, and their degrees are not changed by completing at $\mathfrak{P}$. Thus, the (not necessarily normal) extension KT/T contains a unique subextension V_0/T of degree $[V_0:T] = e_0$ in which $\mathfrak{P}$ is tamely ramified. (See, for example, [5], Theorem 3–4–7, p. 92.) Clearly $V_0 \subseteq V$. Now V/T is a cyclic extension, so V_0/T is also cyclic (thus, in particular, normal).

Let $\pi_K \in K$ and $\pi_{V_0} \in V_0$ be prime elements for $\mathfrak{P}_K$ and $\mathfrak{P}_{V_0}$, respectively. (Then π_K is also a prime element for $\mathfrak{P}_{KT}$ in KT.) If $e_0 \neq 1$, we may choose $\sigma \in \mathrm{Gal}\,(V_0/T)$, $\sigma \neq 1$, and by (1.9) applied to $T \subseteq V_0 \subseteq KT$, we have

$$w_L(\sigma(\pi_{V_0}) - \pi_{V_0}) = \sum_{s \to \sigma} w_L(s(\pi_K) - \pi_K).$$

Now, since V_0/T is a normal extension, totally and tamely ramified at $\mathfrak{P}$,

$$w_L(\sigma(\pi_{V_0}) - \pi_{V_0}) = w_L(\pi_{V_0}) = [KT : V_0] w_L(\pi_K) = p^r(e/n).$$

But, by assumption, $K \equiv K' \pmod{(\mathfrak{P}^{\#})^{(e/n)+1}}$, so that (1.3) implies $w_L(s(\pi_K)-\pi_K) \geq (e/n)+1$. Since there are $[KT : V_0]$ terms in the sum, we have

$$\sum_{s \to \sigma} w_L(s(\pi_K)-\pi_K) \geq p^r((e/n)+1).$$

But this is greater than $w_L(\sigma(\pi_{V_0})-\pi_{V_0})$, which is a contradiction. Hence $e_0 = 1$.

We establish, next, a criterion which will be useful in the exact determination of $M(\mathfrak{P}^{\#}; K, K')$.

(1.10). PROPOSITION. *Let* $n = [K : F] = [K' : F]$, *and suppose* $\mathfrak{P}$ *is totally ramified in* K/F *and* K'/F. *Let* π *be a prime element for* $\mathfrak{P}_K$ *in* K. *Then* $M(\mathfrak{P}^{\#}; K, K')$ *is the largest integer* M *such that* $\pi \equiv \alpha' \pmod{(\mathfrak{P}^{\#})^M}$ *for some* $\alpha' \in \mathfrak{O}_{K'}$.

Proof. Let M be the integer so defined. Clearly $M \geq M(\mathfrak{P}^{\#}; K, K')$. Suppose $M > M(\mathfrak{P}^{\#}; K, K')$. Then, by (1.8), $M > e/n = e(\mathfrak{P}; L/K) = e(\mathfrak{P}; L/K')$. Suppose $\pi \equiv \pi' \pmod{(\mathfrak{P}^{\#})^M}$ where $\pi' \in \mathfrak{O}_{K'}$. Then, since π is exactly divisible by $(\mathfrak{P}^{\#})^{e/n}$, so is π', whence π' is a prime element for $\mathfrak{P}_{K'}$ in $\mathfrak{O}_{K'}$. Now, since $\mathfrak{P}$ is totally ramified in K/F and K'/F, we have $\mathfrak{O}_K + (\mathfrak{P}^{\#})^M = \mathfrak{O}_F[\pi] + (\mathfrak{P}^{\#})^M$ and $\mathfrak{O}_{K'} + (\mathfrak{P}^{\#})^M = \mathfrak{O}_F[\pi'] + (\mathfrak{P}^{\#})^M$. But $\pi \equiv \pi' \pmod{(\mathfrak{P}^{\#})^M}$ implies $\mathfrak{O}_F[\pi'] + (\mathfrak{P}^{\#})^M = \mathfrak{O}_F[\pi] + (\mathfrak{P}^{\#})^M$, whence $K \equiv K' \pmod{(\mathfrak{P}^{\#})^M}$. This contradicts $M > M(\mathfrak{P}^{\#}; K, K')$ so $M = M(\mathfrak{P}^{\#}; K, K')$.

Now, if $\mathfrak{A} = \mathfrak{A}_K \mathfrak{O}_L = \mathfrak{A}_{K'} \mathfrak{O}_L$, as considered in [1], then $\mathfrak{A}$ is surely ambiguous in L/F. (For $\mathfrak{A}$ is invariant under the automorphisms of both Gal (L/K) and Gal (L/K').) Moreover, the lowest common multiple of two ideals of that type is again of that type. Hence we may define:

(1.11) DEFINITION. Let $\mathfrak{m}(K, K')$ denote the (unique) minimal ideal $\mathfrak{A}$ of $\mathfrak{O}_L$ such that $\mathfrak{A} = \mathfrak{A}_K \mathfrak{O}_L = \mathfrak{A}_{K'} \mathfrak{O}_L$ and such that $K \equiv K' \pmod{\mathfrak{A}}$. We note that $\mathfrak{m}(K, K')$ is divisible by all other ideals having these properties.

Clearly $\mathfrak{m}(K, K')$ is the highest divisor $\mathfrak{A}$ of (i.e. smallest ideal $\mathfrak{A}$ containing) $\mathfrak{M}(K, K')$ with the property $\mathfrak{A} = \mathfrak{A}_K \mathfrak{O}_L = \mathfrak{A}_{K'} \mathfrak{O}_L$. We will regard $\mathfrak{m}(K, K')$ at various times as an ideal of $\mathfrak{O}_K$ or of $\mathfrak{O}_{K'}$ or of $\mathfrak{O}_L$. We note the following corollary to (1.7) and (1.8).

(1.12) COROLLARY. *If* $[K : F] \neq [K' : F]$, $\mathfrak{m}(K, K') = (1)$. *Suppose* $[K : F] = [K' : F] = n$, *and let* $\mathfrak{p}$ *be a prime divisor of* F.

(i) *If* $\mathfrak{p}$ *is not totally ramified in* K/F *and* K'/F, *then* $\mathfrak{p}$ *is relatively prime to* $\mathfrak{m}(K, K')$.

(ii) *If* $\mathfrak{p}$ *is totally ramified in* K/F *and* K'/F, *then* $\mathfrak{P}_K | \mathfrak{m}(K, K')$. *Moreover,* $\mathfrak{m}(K, K')$ *is divisible by* $(\mathfrak{P}_K)^2$ *only if* $n = p^r$ *for some* r, *where* p *is the rational prime divisible by* $\mathfrak{p}$.

Proof. (i) is immediate from (1.7). To show the first assertion suppose $n > n'$. If $\mathfrak{p}$ is totally ramified in K/F and K'/F, suppose $(\mathfrak{P}^{\#})^s$ is the power of $\mathfrak{P}^{\#}$ dividing $\mathfrak{m}(K, K')$, and $s > 0$. Then, by (1.7), $s \leq e/n < e/n'$, and $(\mathfrak{P}^{\#})_K^s = \mathfrak{P}_K$ and $(\mathfrak{P}^{\#})_{K'}^s = \mathfrak{P}_{K'}$. But we must have $(\mathfrak{P}^{\#})^s = \mathfrak{P}_K \cdot \mathfrak{O}_L = \mathfrak{P}_{K'} \cdot \mathfrak{O}_L$ which implies $s = e/n = e/n'$, a contradiction. Thus $n = n'$, which proves the first assertion. Moreover, if $n = n'$, $(\mathfrak{P}_K)\mathfrak{O}_L = (\mathfrak{P}_{K'})\mathfrak{O}_L = (\mathfrak{P}^{\#})^{e/n}$, so that $\mathfrak{m}(K, K')$ is divisible exactly by $(\mathfrak{P}_K)^m$ where m is the largest integer such that $m \cdot (e/n) \leq M(\mathfrak{P}^{\#}; K, K')$. Clearly, (1.8) implies that $m \geq 1$ with $>$ holding only if $n = p^r$ for some r. This proves (ii).

We shall henceforth denote by $m(\mathfrak{P}_K; K, K')$ the largest integer m such that $(\mathfrak{P}_K)^m$ divides $\mathfrak{m}(K, K')$ and we record here the observation

$$m(\mathfrak{P}_K; K, K') = \left[\frac{M(\mathfrak{P}^{\#}; K, K')}{e(\mathfrak{P}; L/K)}\right] \tag{1.13}$$

where the brackets denote the greatest integer function.

2. Normal Extensions

Let L/F be any normal extension of F, and $\mathfrak{p}$ a prime divisor of F. Let $\mathfrak{P}$ be a prime divisor of L lying over $\mathfrak{p}$. Denote by $G_i(\mathfrak{P}; L/F)$ the ith ramification group of $\mathfrak{P}$ in L/F, where the numbering is chosen so that G_{-1} is the decomposition group, G_0 is the inertia group, and $\sigma \in G_i$ if and only if $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{i+1}}$ for all $\alpha \in \mathfrak{O}_L$. This is the numbering used in [4] and [5], but it differs from that used in [1] and [3]. If $\mathfrak{p}$ is totally ramified in L/F, denote by $t(\mathfrak{p}; L/F)$ the largest integer t such that $G_t(\mathfrak{P}; L/F) = \mathrm{Gal}\,(L/F)$. We shall omit the reference to the prime in the notation, when it can be inferred from the context. (The "order of ramification" v used in [1] and [3] is the smallest integer v such that $G_v = \{1\}$. In particular, when L/F is cyclic of prime degree, $v = t+1$).

Now, suppose K/F and K'/F are normal extensions, $F = K \cap K'$, and let $L = K \cdot K'$, the composite. Also suppose $[K : F] = [K' : F]$. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_F$, totally ramified in K/F and in K'/F. Let $\mathfrak{P}$ be a prime factor of $\mathfrak{p}$ in $\mathfrak{O}_L$. The following is a restatement of ([1], Theorem 7).

(2.1) Proposition. $M(\mathfrak{P}^{\#}; K, K') \leq e(\mathfrak{P}; L/K) \cdot (t+1)$ *and* $m(\mathfrak{P}_K; K, K') \leq (t+1)$ *where* $t = \min(t(\mathfrak{p}; K/F), t(\mathfrak{p}; K'/F))$.

Proof. Let $t = t(K/F) \leq t(K'/F)$. Choose $\sigma \in \mathrm{Gal}\,(K/F)$, $\sigma \notin G_{t+1}(\mathfrak{P}_K; K/F)$. Then, there is an $\alpha \in \mathfrak{O}_K$ such that $\sigma(\alpha) - \alpha$ is exactly divisible

by $\mathfrak{P}_K^{t+1}$. Since, by (1.3), $\mathfrak{M}(K,K')|\sigma(\alpha)-\alpha$, and $\mathfrak{P}_K\mathfrak{O}_L = (\mathfrak{P}^{\#})^{e(\mathfrak{P};\,L/K)}$, we must have $M(\mathfrak{P}^{\#};\,K,K') \leq e(\mathfrak{P};\,L/K)\cdot(t+1)$. By (1.13), $m(\mathfrak{P}_K;\,K,K') \leq (t+1)$.

Suppose now that $e(\mathfrak{P};\,L/K)=1$, which is to say that $\mathfrak{P}_K\cdot\mathfrak{O}_L = \mathfrak{P}^{\#}$. (Also $\mathfrak{P}_{K'}\mathfrak{O}_L = \mathfrak{P}^{\#}$, since $e(\mathfrak{P};\,L/K) = e(\mathfrak{P};\,L/K')$.) We intend to show that both inequalities in (2.1) become equalities. Let T = the inertia field for $\mathfrak{P}$ in L/F. Then $[T:F]=[K:F]$. Also, since $\mathfrak{P}$ is unramified in T/F, we have $T\cap K = F$. Thus, the map $\sigma\to\sigma|_K$ from Gal (L/T) to Gal (K/F) is an isomorphism. (Of course, the same holds for K'/F as well.)

(2.2) PROPOSITION. *If* $e(\mathfrak{P};\,L/K)=1$, *the canonical isomorphism* Gal $(L/T)\cong$ Gal (K/F) *maps* $G_i(\mathfrak{P};\,L/T)$ *onto* $G_i(\mathfrak{P}_K;\,K/F)$ *for all* i. *In particular,* $t(\mathfrak{p};\,K/F) = t(\mathfrak{P}_T;\,L/T)$.

Proof. Let π be a prime element for $\mathfrak{P}_K$ in K. Then π is a prime element for $\mathfrak{P}$ in L. Moreover, if $\sigma\in$ Gal (L/T), then $\mathfrak{P}^{i+1}|\sigma(\pi)-\pi$ if and only if $\mathfrak{P}_K^{i+1}|\sigma(\pi)-\pi$, since $\sigma(\pi)-\pi\in K$. Hence $\sigma\in G_i(\mathfrak{P};\,L/T)$ if and only if $\sigma|_K\in G_i(\mathfrak{P}_K;\,K/F)$. The rest is clear.

(2.3) THEOREM. *If* $e(\mathfrak{P};\,L/K)=1$, *then*

$$M(\mathfrak{P}^{\#};\,K,K') = t+1 = m(\mathfrak{P}_K;\,K,K')$$

where $t = t(\mathfrak{p};\,K/F) = t(\mathfrak{p};\,K'/F)$.

Proof. From (2.2) applied to K/F and to K'/F, it follows that $t(\mathfrak{p};\,K/F) = t(\mathfrak{p}:\,K'/F)$. For any subfield E of L, let $\bar{E}$ denote the residue class field $\mathfrak{O}_E/\mathfrak{P}_E$. Choose a system of representatives A of $\bar{L}$ such that those elements of A which represent classes of $\bar{F}$ are chosen in F. Let $\pi\in K$ be a prime element for $\mathfrak{P}_K$. Then π is a prime element for $\mathfrak{P}$. Hence, in the usual way, for any integer s, each element of $\mathfrak{O}_L$ is congruent (mod $\mathfrak{P}^{s+1}$) to a (unique) element of form

$$\sum\{a_i\pi^i : i=0,\ldots,s\}$$

where $a_i\in A$. Let α' be any element of $\mathfrak{O}_{K'}$ and suppose

$$\alpha' \equiv \sum\{a_i\pi^i : i=0,\ldots,t\} \pmod{\mathfrak{P}^{t+1}}. \tag{2.4}$$

We intend to show first that each $a_i\in F$.

Now $a_0\in F$, since $\bar{K}'=\bar{F}$. Let σ be any element of the decomposition group $G_{-1}(\mathfrak{P};\,L/K)$. Then $\sigma(\mathfrak{P})=\mathfrak{P}$, $\sigma|_K=1$, and $\sigma|_{K'}\in G_t(K'/F)$. Thus

$$\alpha' \equiv \sigma(\alpha') \pmod{\mathfrak{P}_{K'}^{t+1}},$$

and applying σ to both sides of (2.4),

$$\sigma(\alpha') \equiv \sum\{\sigma(a_i)\pi^i : i=0,\ldots,t\} \pmod{\mathfrak{P}^{t+1}}.$$

Thus,

$$\sum \{a_i\pi^i : i = 0,\ldots,t\} \equiv \sum \{\sigma(a_i)\pi^i : i = 0,\ldots,t\} \pmod{\mathfrak{P}^{t+1}}. \quad (2.5)$$

Since $a_0 \in F$, $a_0 = \sigma(a_0)$. Thus, subtracting the first term from both sides of (2.5) and dividing by π, we see that $a_1 \equiv \sigma(a_1) \pmod{\mathfrak{P}}$. Now, the decomposition group $G_{-1}(\mathfrak{P}; L/K)$ is canonically identified with $\mathrm{Gal}(\bar{L}/\bar{K}) = \mathrm{Gal}(\bar{L}/\bar{F})$. As σ runs over $G_{-1}(\mathfrak{P}; L/K)$, we see that the residue class of a_1 is fixed under all automorphisms of $\bar{L}/\bar{F}$, and hence belongs to $\bar{F}$. Thus $a_1 \in F$, by the choice of A. Hence $a_1 = \sigma(a_1)$. Thus, subtracting $a_0 + a_1\pi$ from both sides of (2.5) and dividing by π^2, we obtain $a_2 \equiv \sigma(a_2) \pmod{\mathfrak{P}}$. The same argument shows $a_2 \in F$ so $a_2 = \sigma(a_2)$. Proceeding in this way, we show eventually that $a_i \in F$ for $i = 0,\ldots,t$. Hence

$$\sum \{a_i\pi^i : i = 0,\ldots,t\} \in \mathfrak{O}_K$$

and, by (2.4), we have

$$\alpha' \equiv \alpha \pmod{\mathfrak{P}^{t+1}} \text{ for some } \alpha \in \mathfrak{O}_K. \quad (2.6)$$

Now, choose any $\sigma \in \mathrm{Gal}(L/K)$. Then $\sigma|_{K'} \in G_t(K'/F)$, so $\alpha' \equiv \sigma(\alpha') \pmod{\mathfrak{P}_{K'}^{t+1}}$. But applying σ to (2.6), we get $\sigma(\alpha') \equiv \alpha \pmod{\sigma(\mathfrak{P})^{t+1}}$. Thus $\alpha' \equiv \alpha \pmod{\sigma(\mathfrak{P})^{t+1}}$. As σ runs over $\mathrm{Gal}(L/K)$, $\sigma(\mathfrak{P})$ runs over all conjugates of $\mathfrak{P}$. Hence $\alpha' \equiv \alpha \pmod{(\mathfrak{P}^{\#})^{t+1}}$, and $\mathfrak{O}_{K'} \subseteq \mathfrak{O}_K + (\mathfrak{P}^{\#})^{t+1}$. By symmetry, $K \equiv K' \pmod{(\mathfrak{P}^{\#})^{t+1}}$, and so $M(\mathfrak{P}^{\#}; K, K') \geq t+1$. By (2.1), equality holds. By (1.13), $m(\mathfrak{P}_K; K, K') = t+1$, which completes the proof.

3. Cyclic Extensions of Prime Degree

Now, suppose K/F and K'/F are cyclic extensions of prime degree p, and $\mathfrak{p}$ is a prime of $\mathfrak{O}_F$, dividing p and totally ramified in K/F and K'/F, and $\mathfrak{P}$ a prime divisor of $\mathfrak{p}$ in $\mathfrak{O}_L$, where $L = K \cdot K'$. Then $e = e(\mathfrak{P}; L/F) = p$ or p^2.

(3.1) Theorem.

$$\text{Let } t = \min(t(\mathfrak{p}; K/F), t(\mathfrak{p}; K'/F)).$$

$$\text{Let } t_1 = \begin{cases} t(\mathfrak{p}; L/F) \text{ if } e = p^2, & \text{or} \\ -1 \text{ if } e = p. \end{cases}$$

Then

(i) $M(\mathfrak{P}^{\#}; K, K') = \begin{cases} t+1 \text{ if } e = p, & \textit{and} \\ p(t+1) - t_1 \text{ if } e = p^2. & (\textit{In this case } p \nmid t_1). \end{cases}$

(ii) $m(\mathfrak{P}_K; K, K') = \left[\dfrac{p(t+1)-t_1}{p}\right] = \left[\dfrac{p(t+1)-(t_1+1)}{p}\right].$

Proof. Let $M = M(\mathfrak{P}; K, K')$. We first prove (i).

If $e = p$, then $e(\mathfrak{P}; L/K) = 1$, and the result follows from (2.3). Suppose $e = p^2$, whence $\mathfrak{P}^{\#} = \mathfrak{P}$. Let π be a prime element for $\mathfrak{P}_K$ in K. Then $\pi \equiv \pi' \pmod{\mathfrak{P}^M}$ for some prime element π' for $\mathfrak{P}_{K'}$ in K', and $\pi \not\equiv \pi' \pmod{\mathfrak{P}^{M+1}}$, by (1.10). Thus, $\pi = \pi' + \alpha$ where $w_L(\alpha) = M$.

Now, since $\bar{L} = \bar{F}$, we have $p \nmid M$. (Otherwise, $\alpha \equiv a(\pi')^{M/p} \pmod{\mathfrak{P}^{M+1}}$ for some $a \in F$, whence $\pi \equiv \pi' + a(\pi')^{M/p} \pmod{\mathfrak{P}^{M+1}}$. This implies $M(\mathfrak{P}; K, K') > M$, a contradiction.) Let σ generate $\mathrm{Gal}(L/K')$. Then

$$\sigma(\pi) - \pi = \sigma(\alpha) - \alpha.$$

Now $w_K(\sigma(\pi) - \pi) = t(K/F) + 1$, since $\sigma|_K$ generates $\mathrm{Gal}(K/F)$. By ([4], Exercise 3a, p. 79), $w_L(\sigma(\alpha) - \alpha) = t(L/K') + M$, since $p \nmid M$. Thus, $p \cdot (t(K/F) + 1) = t(L/K') + M$, so

$$M = p \cdot (t(K/F) + 1) - t(L/K'). \tag{3.2}$$

Similarly, reversing the roles of K and K', we see that $M = p \cdot (t(K'/F) + 1) - t(L/K)$, whence

$$t(L/K') - t(L/K) = p \cdot (t(K/F) - t(K'/F)). \tag{3.3}$$

Now, the form of (3.2) is similar to the form of the result in (i) which we are proving. It remains only to establish certain relationships between the ramification invariants.

Let π_L be a prime element for $\mathfrak{P}$ in L. Suppose that $G_{t_1+1}(L/F) = \{1\}$. Then if $s \in \mathrm{Gal}(L/F)$, $s \neq 1$, we have

$$w_L(s(\pi_L) - \pi_L) = t_1 + 1. \tag{3.4}$$

Hence $t_1 = t(L/K) = t(L/K')$. Thus, by (3.3), $t(K/F) = t(K'/F) = t$, and (3.2) implies that (i) holds in this case.

Suppose $G_{t_1+1}(L/F) \neq \{1\}$, and let R be the fixed field of $G_{t_1+1}(L/F)$. The Hilbert sequence for L/F is

$$G_0 = G_1 = \ldots = G_{t_1} \supsetneq G_{t_1+1} = \ldots = G_{t_2} \supsetneq G_{t_2+1} = \{1\}$$

for some integer $t_2 > t_1$. If $s \in \mathrm{Gal}(L/F)$, $s \neq 1$, we have

$$w_L(s(\pi_L) - \pi_L) = \begin{cases} t_1 + 1 & \text{if } s \notin \mathrm{Gal}(L/R) \\ t_2 + 1 & \text{if } s \in \mathrm{Gal}(L/R). \end{cases} \tag{3.5}$$

Suppose $R \neq K$ and $R \neq K'$. Then $t(L/K) = t(L/K') = t_1$, so by (3.3) $t(K/F) = t(K'/F) = t$. Hence (3.2) implies that (i) holds in this case. If $R = K$ or $R = K'$, we may suppose (by symmetry) that $R = K$. Then by (3.5), $t(L/K) = t_2 > t_1 = t(L/K')$, whence by (3.3), $t = t(K/F) < t(K'/F)$. Hence (3.2) again implies that (i) holds in this case. This completes the proof of (i).

We note that (ii) holds if $e = p$, by (2.3) and the definition of t_1. If $e = p^2$, then by (1.13), $m(\mathfrak{P}_K; K, K') = [M/p]$, where $M = p(t+1) - t_1$. But, as we noted before, $p \nmid M$, whence $[M/p] = [(M-1)/p]$ and (ii) follows.

For aesthetic and computational reasons, we include at this point three additional facts relating the ramification invariants of the various subextensions of L/F, in the case that $e = p^2$.

(i) $t_1 = t$ if $G_{t_1+1}(L/F) = \{1\}$.
(ii) $t_1 = t(R/F)$ if $G_{t_1+1}(L/F) \neq \{1\}$. (3.6)
(iii) $t_1 \leq t$ in either case.

These facts follow in various easy ways from results in Chapter IV of [4]. We will derive them from (1.9).

If $G_{t_1+1}(L/F) = \{1\}$, let $\sigma \in \mathrm{Gal}\,(K/F)$, $\sigma \neq 1$, and let π_K be a prime element for $\mathfrak{P}_K$ in K. Then

$$w_L(\sigma(\pi_K)-\pi_K) = \sum_{s\to\sigma} w_L(s(\pi_L)-\pi_L).$$

There are exactly p automorphisms s of L/F which restrict to σ. Hence, computing both sides and using (3.4), we get $p\cdot(t(K/F)+1) = p(t_1+1)$, whence (i) follows.

If $G_{t_1+1}(L/F) \neq \{1\}$, let $\sigma \in \mathrm{Gal}\,(R/F)$, $\sigma \neq 1$. A similar computation, using (3.5), gives $p\cdot(t(R/F)+1) = p(t_1+1)$, whence (ii) follows.

In either case, let K be any intermediate field of degree p over F, and let $\sigma \in \mathrm{Gal}\,(K/F)$, $\sigma \neq 1$. Then (1.9) and (3.4) or (3.5) imply similarly that $p\cdot(t(K/F)+1) \geq p(t_1+1)$, whence (iii) follows.

4. Kummer Extensions of Degree p

In addition to the assumptions of Section 3, we suppose that F contains ζ, a primitive pth root of unity. Then $K = F(\mu^{1/p})$ and $K' = F((\mu')^{1/p})$ with $\mu, \mu' \in \mathfrak{O}_F$, and we may assume that $w_F(\mu) = 0$ or 1 and $w_F(\mu') = 0$ or 1 (see [2], Section 39]). Let $w_F(1-\zeta) = a$. The main result of Butts and Mann for extensions of this type is ([1], Theorem 14) which we state as follows:

(4.1) Theorem. *Let* $t = \min(t(\mathfrak{p}; K/F),\ t(\mathfrak{p}; K'/F))$. *Then* $(t+1)-a \leq m(\mathfrak{P}_K; K, K') \leq t+1$.

Proof. The second inequality is clear. We will show the first inequality. In ([2], Section 39] it is shown that $\mathfrak{p}$ is ramified in K/F if and only if either:

(i) $w(\mu) = 1$, or
(ii) $w(\mu) = 0$ and the congruence $x^p \equiv \mu \pmod{\mathfrak{p}^{ap}}$ has no solution in $\mathfrak{O}_F$.

It is further shown in ([1], Theorems 9 and 12) that $t(K/F) = ap-k$ where we have in these same two cases, respectively:

(i) $k = 0$, or
(ii) $k > 0$ and the congruence $x^p \equiv \mu$ is solvable in $\mathfrak{O}_F$ modulo $\mathfrak{p}^k$, but not mod $\mathfrak{p}^{k+1}$.

Suppose $t = t(K/F)$. Since by (3.6)(iii), $t_1 \leq t = ap-k$, we have by (3.1)(ii),

$$m(\mathfrak{P}_K; K, K') = [t+1-(t_1)/p] \geq [t+1-(ap-k)/p]$$
$$= t+1-a+[k/p].$$

(We remark that the term $[k/p]$ gives an improvement of the result stated in ([1], Theorem 14]; however this improvement is implicit in the proof given in [1]).

Note that we always have $m = m(\mathfrak{P}_K; K, K') \leq ap+1$. As a final application, we determine necessary and sufficient conditions for $m = ap+1$ and for $m = ap$. Our conditions substantially simplify the complicated congruence conditions of ([1], Theorem 16) and generalize those of ([1], Theorem 17).

In order for m to be $\geq ap$, clearly we must have $t(K/F)+1 \geq ap$ or $t(K/F) \geq ap-1$, and similarly $t(K'/F) \geq ap-1$. Thus, we must have either $w_F(\mu) = 0$ and the congruence $x^p \equiv \mu \pmod{\mathfrak{p}^2}$ not solvable, or $w_F(\mu) = 1$. Similarly for μ'.

(4.2) THEOREM. *Let $m = m(\mathfrak{P}_K; K, K')$. Suppose $t(K/F)$ and $t(K'/F)$ are $\geq ap-1$. Then the following hold.*

(i) *$m = ap+1$ if and only if $w_F(\mu) = w_F(\mu') = 1$ and the congruence $\mu x^p \equiv \mu' \pmod{\mathfrak{p}^{ap+1}}$ is solvable in $\mathfrak{O}_F$.*

(ii) *$m = ap$ if and only if either of the following holds:*

(a) *$w_F(\mu) = w_F(\mu') = 1$ and the congruence $\mu x^p \equiv \mu'$ is solvable in $\mathfrak{O}_F$ modulo $\mathfrak{p}^{ap+1-p}$, but not $\bmod \mathfrak{p}^{ap+1}$.*

(b) *$w_F(\mu) = w_F(\mu') = 0$ and the congruence $\mu x^p \equiv (\mu')^r \pmod{\mathfrak{p}^{ap}}$ is solvable in $\mathfrak{O}_F$, for some r with $0 < r < p$.*

Proof. (i). Now $m = [(t+1)-(t_1)/p] \leq t+1 \leq ap+1$. Thus, $m = ap+1$ if and only if $t = ap$ and $t_1 = -1$ (since $t_1 = 0$ is impossible). Now, $t = \min(t(K/F), t(K'/F)) = ap$ if and only if $w_F(\mu) = w_F(\mu') = 1$, so we suppose $t = ap$. Next, $t_1 = -1$ if and only if $e = p$, or equivalently $[T:F] = p$, where T is the inertia field for $\mathfrak{P}$ in L/F. The intermediate fields of degree p over F are (besides K and K') the fields $F((\mu'\mu^s)^{1/p})$ for $s = 1, \ldots, p-1$. The prime $\mathfrak{p}$ is ramified in all of these with the possible exception of the last ($s = p-1$). Thus $t = -1$ if and only if $\mathfrak{p}$ is unramified in $F((\mu'/\mu)^{1/p})$ over F. This is equivalent to solvability of the congruence $x^p \equiv \mu'/\mu \pmod{\mathfrak{p}^{ap}}$ in $\mathfrak{O}_F$, which is equivalent to $\mu x^p \equiv \mu' \pmod{\mathfrak{p}^{ap+1}}$, since $w_F(\mu) = 1$. (One may assume here, for convenience, that $\mathfrak{O}_F$ is the valuation ring for $\mathfrak{p}$ in F.)

(ii). Using the same inequality as in the proof of (i), we see that $m = ap$ if and only if either of the following occur:

(a′) $t = ap$ and $0 < t_1 \leq p$.

(b′) $t = ap-1$ and $t_1 = -1$ (since $t_1 = 0$ is impossible).

Considering (a′), we see $t = ap$ if and only if $w_F(\mu) = w_F(\mu') = 1$, so we suppose $t = ap$. Now if $0 < t_1 \leq p$, then $t_1 < t$ and (in (3.6)) we must have $t(R/F) = t_1$, for some intermediate field R of degree p over F. As in the proof of (i), the only possibility for R is $F((\mu'/\mu)^{1/p})$. Then $t(R/F) = ap-k$ where the congruence $x^p \equiv \mu'/\mu$ is solvable mod $\mathfrak{p}^k$ but not mod $\mathfrak{p}^{k+1}$. The condition $0 < t_1 \leq p$ then becomes $0 < ap-k \leq p$ or $ap-p \leq k < ap$. Thus, $0 < t_1 \leq p$ is equivalent to solvability of the congruence $\mu x^p \equiv \mu'$ modulo $\mathfrak{p}^{ap+1-p}$, but not mod $\mathfrak{p}^{ap+1}$. Thus (a′) is equivalent to (a).

Now, assume (b′). By (2.3), $t_1 = -1$ implies that $t = t(K/F) = t(K'/F)$. Thus $t = ap-1$ implies $w_F(\mu) = w_F(\mu') = 0$. The condition $t_1 = -1$ implies that $\mathfrak{p}$ is unramified in one of the intermediate fields, say $F(((\mu')^r/\mu)^{1/p})$ where $0 < r < p$. This implies that $x^p \equiv (\mu')^r/\mu \pmod{\mathfrak{p}^{ap}}$ is solvable, or equivalently $\mu x^p \equiv (\mu')^r \pmod{\mathfrak{p}^{ap}}$. Conversely, if $w_F(\mu) = w_F(\mu') = 0$, solvability of this congruence implies $t_1 = -1$. Moreover, under our general assumption that $t \geq ap-1$, $w_F(\mu) = w_F(\mu') = 0$ implies $t = ap-1$. Hence (b′) is equivalent to (b).

References

1. Butts, H. S. and Mann, H. B. Corresponding residue systems in algebraic number fields. *Pacific J. Math.* **6** (1956), 211–224.
2. Hecke, E. "Vorlesungen über die Theorie der algebraischen Zahlen". Leipzig, 1923.
3. Mann, H. B. "Introduction to Algebraic Number Theory". Columbus, Ohio, 1955.
4. Serre, J.-P. "Corps Locaux". Paris, 1962.
5. Weiss, E. "Algebraic Number Theory". New York, 1963.